스마트 팩토리 디바이스의 보안 취약성 분석

이용주* · 우성희**

*충북대학교, **한국교통대학교

Analysis of Vulnerability of Devices in Smart Factory

Yong-Joo Lee* · Sung-Hee Woo**

*ChungBuk National University, **Korea National University of Transportation

E-mail : *silvianna7@naver.com, **shwoo@ut.ac.kr

요 약

4차 산업의 혁명과 함께 스마트 팩토리에 대한 관심도 고조되고 있다. 그러나 최근 몇 년 사이에 스마트 팩토리의 디바이스에 대한 보안 위협이 늘고 있어, 보안 취약성 문제로 인한 기업 데이터유출 문제가 우려 사항으로 지적되고 있다. 본 논문에서는 스마트 팩토리에서 필요한 보안 요구사항을 크게 네 가지로 나누어 분석하고 이중에서도 디바이스에 관련된 보안 취약점 등을 분석하고 최근 새로이 발생하여 급증하는 공격 유형에 대해서도 논의하고자 한다.

ABSTRACT

The concern about Smart Factory has increased according to the 4th revolution. The number of security threats targeting Smart Factory devices has increased over the last years and it is possible to cause the vulnerability of security about industry secret data. In this paper, we devide security requirements into four and analyze security vulnerability of Smart Factory devices and describe the attack type newly happened.

키워드

Smart Factory, Security, Attack

Ⅰ. 서 론

최근 활발히 연구되고 있는 4차 산업 혁명은 독일을 중심으로 산업 및 학계에서 가장 빈번하게 협의되는 주제 중 하나로서, 독일 연방 정부가 독일 제조산업의 경쟁력 확보를 위해 2011년 하이테크 전략의 핵심적인 이니셔티브 중 하나로서 인더스트리 4.0을 발표한 이후, 많은 논문과 리포트가 4차 산업혁명에 초점을 맞추고 있다. 4차 산업혁명의 발의는 독일이 시작하였으나 최근에는 미국과 중국을 포함하여, 일본, 영국, 싱가폴 등 많은 국가를 중심으로 제조혁신 관련 어젠다를 발표하고 있다. 우리나라에서도 갈수록 떨어지는 국내 제조업의 경쟁력을 높이는 유일한 기술로 평가되어 정부, 연구소, 대학 등을 중심으로 많은 연구가 이루어지고 있다. 특히 산업부의 스마트 팩토리 연구/개발 지원책이 대표적인 사례라고 할 수 있다. 그러나 활발한 연구에 대해 실제 제조현장에서 그다지 활발하게 수용되지 못하고 있는데 이는 투자 금액에 대한 부담과 산업기밀의 중요성에 비해 취약한 보안기술이 그 이유로 거론되고 있다. 본 논문에서는 이러한 인터스트리 4.0의 핵심 기술인 스마트 팩토리에 대해 살펴보고 가장 공격이 많이 일어나는 스마트 팩토리의 디바이스에 초점을 맞추어 환경을 분석하고 보안 취약점을 분석하여 이에 대한 대응책을 제시하고자 한다[1].

Ⅱ. 본 론

1. 인더스트리 4.0과 스마트 팩토리

인더스트리 4.0은 임베디드 시스템 생산 기술과 스마트 생산 프로세스를 결합하여 제조업과 관련 산업의 가치사슬 및 비즈니스 모델을 획기적으로 변화시키기 위한 시도이며 이러한 가치가 실제로 구현되는 플랫폼을 스마트 팩토리라고 정의하였다. 중앙 집중형 생산에서 분산형 생산으로의 패러다임 전환을 통해 전통적인 생산 방식을 탈피하고자 함이다. 그림 1은 사물인터넷과 사물인터넷 응용과의 관계를 보여주고 있다.

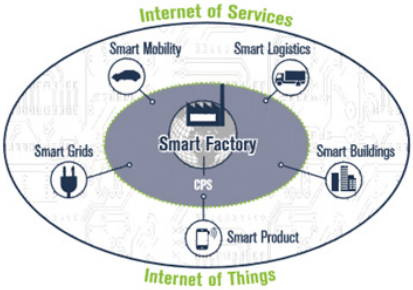

그림 1. 사물인터넷과 스마트팩토리

2. 스마트 팩토리 주요 이슈

스마트 팩토리의 구현을 위한 주요 이슈로는 표준화, 효율적 관리, 통신인프라, 보안 등이 있다. 표준화는 제조공정의 복잡도에 의해 다양한 구성요소 들이 결합되어 있어, 이들의 유기적 연계를 통한 정보 전달과 가공에 의해 지능화, 효율화, 안전화, 친환경화가 이루어지고 정보의 전달과 가공이 표준을 통해 이루어져야 한다. 표준화 다음으로 중요하게 접근해야할 이슈는 보안이다. 표준화가 될수록 가장 중요해지는 기술이 보안이며 스마트 팩토리가 구축이 되면 기존보다 상상을 초월할 데이터가 축적되게 되고, 분석 할 수 있게 된다. 이런 경우 데이터가 유출되면 기업에게 더 큰 재앙으로 다가올 수 있다. 또한 외부 네트워크의 악성 소프트웨어 침입 및 사이버 공격의 위험성이 높아지게 되어 안전과 보안에 대한 문제가 해결되는 것이 무엇보다 중요하다. 제조업과 통신기술을 융합하여 전환시키기 위해서 통신 인프라 장비 또한 신뢰성이 높아야 하며 기기간의 연결이 끊임없이 지속되어야 한다. 이러한 기계와 설비가 소프트웨어의 도움을 받아 지능적으로 상호 통신과 작업 시스템을 협업 네트워크로 연결하게 되어 내부뿐 아니라 외부에서도 동적 관리를 위한 네트워킹이 이루어 져야한다. 따라서 이러한 복잡한 시스템을 효율적으로 관리하기 위한 기술 또한 중요한 하나의 이슈로 자리 잡고 있다. 본 논문에서는 이러한 이슈 중에서 안전과 보안에 대한 이슈에 대해서 다루고자 한다[2].

3. 스마트 팩토리의 디바이스통신

스마트 팩토리는 사물인터넷, 빅데이터, 클라우드, CPS(Cyber Physical System) 스마트센서, 3D 프린팅 등 다양한 ICT 기술과 제품의 기획, 설계, 생산, 유통, 판매 등 제조 전 과정이 지능적으로 융합된 산업이라고 볼 수 있다. 또한 개별 공장의 설비 및 공정이 생산네트워크로 연결되고 모든 생산, 데이터, 정보가 자동화 및 정보화 되어 가치사슬 전체가 실시간 연동, 통합된 시스템으로 구성된다. 이러한 통합된 시스템으로 연동되기 위해 각각의 디바이스들은 센서 등이 부착되어 M2M(Machine2Machine) 네트워크로 연결되어 연동된다. M2M 통신은 디바이스들이 유무선 네트워크를 통하여 통신할 수 있게 해주는 기술을 의미한다. 디바이스들은 센서 등을 이용하여 이벤트가 발생하였을 때 M2M 게이트웨이를 이용하여 네트워크 도메인으로 전달한다. 이러한 M2M 통신을 가능하게 하는 기술로 현재 표준화가 진행되는 기술로는 RFID, mobile internet wired&wireless 통신, IPv4/IPv6, ZigBee, 6LoWPAN, Bluetooth Low Energy 등이 있다. 그림 2에서 M2M 게이트웨이는 디바이스들이 코어네트워크로 연결되기 위해 사용된다. 따라서 사물인터넷은 IP 기반의 디바이스 혹은 IP 기반이 아닌 디바이스가 이질적인 네트워크에서 서로 연결되는 환경이 된다. 그림 3는 다양한 종류의 디바이스들이 이질적인 네트워크에서 함께 연동되는 M2M 통신을 보여주고 있다[3].

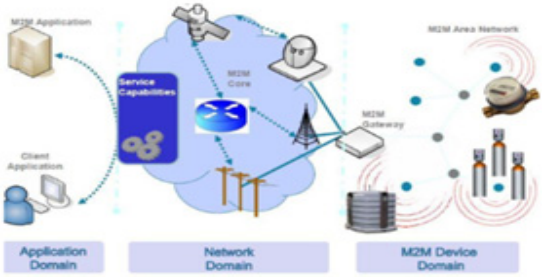

그림 2. 스마트 팩토리 네트워크

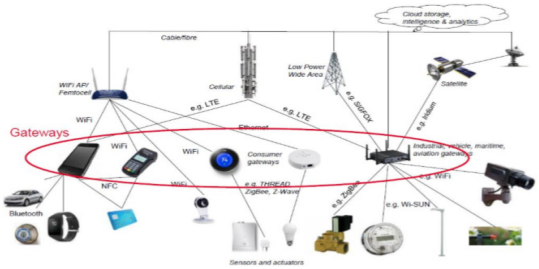

그림3. M2M 디바이스의 통합망

4. 스마트 팩토리의 보안 기술 분석

스마트 팩토리의 인프라 및 서비스는 대부분 기존 산업 제어 시스템/네트워크에 기반을 두면서 인터넷과 연동된다. 이 때문에, 스마트공장의 다양한 구성요소(센서/디바이스,네트워크,플랫폼, 애플리케이션) 보안 취약성과 레거시 산업 네트워크와 연동시의 보안 취약성, 플랫폼 연동시의 보안 취약성 등이 중요한 이슈가 된다. 각 요소별 보안 기술에 대해 살펴보면 다음과 같다.

1) 센서 디바이스 보안기술

스마트 팩토리용 센서와 디바이스는 오픈소스 하드웨어 형태의 디바이스에서 대형 공장 장비까지 매우 다양한 크기와 특성을 가진다. 하지만, 기본적으로 이러한 스마트 팩토리에서 사용되는 디바이스는 기능과 통신/네트워크, 하드웨어와 소프트웨어 관점에서의 특성은 유사하기 때문에 기존의 인터넷상의 디바이스가 갖는 보안 취약성

과 동일한 형태의 보안 취약성을 갖는다.

2) 네트워크보안기술

스마트 팩토리 네트워크는 디바이스와 연결되는 구간인 M2M 통신 구간과 어플리케이션 및 서비스가 연결되는 구간의 네트워크로 구분되는데 특히 팩토리 내부의 프로토콜을 상황에 맞게 재구성하는 경우가 늘고 있다. 이에 특화된 보안 프로토콜이 필요하며 공격 감지기술 등이 요구된다.

3) 플랫폼 보안기술

플랫폼 보안에 대한 요구사항은 각종 센서와 디바이스가 연동되어 수신되는 데이터를 저장/가공/분석/연동하기 위한 보안이 가장 중요한 요소가 된다. 이러한 플랫폼에서는 각종 디바이스/네트워크에서 제공하는 보안기술과 연동할 수 있는 보안 에이전트와 플랫폼 자체에서 인증/인가/접근제어기능을 갖는 보안기술, 기업 프라이버시 보호기술, 서비스 연동시의 보안연관/인증/인가/접근제어, 데이터연동시의 보안 기술 등이 필요하다.

4) 애플리케이션 보안 기술

스마트 팩토리 애플리케이션은 제조 설비와 각종 산업용 통신/네트워크, 제조서비스용 프레임워크, 각종 제조 애플리케이션 융복합 통합 센싱/운영/제어 되는 서비스 환경이다. 이 때문에 이에 대한 기밀성, 무결성 제공뿐만 아니라, 접근제어, 보안관리, 보안정책, 취약성 대응/침해 대응, 보안관제/물리보안, 위험관리, 신뢰성보장, ID 식별관리 등에 대한 보안이 필요하다[4].

5. 디바이스의 보안취약성 분석

기존의 산업제어 시스템 통신은 IP 기반의 인터넷이 연결됨에 따라 보안 취약성이 매우 높아지게 되었다. 스마트 팩토리 역시 산업 제어 시스템을 기반으로 하고 있기 때문에 기존의 산업 제어 시스템이 가지는 보안 요구사항과 보안 취약성을 모두 가지게 된다. 그중 최근에는 디바이스에서 발생하는 데이터 등의 산업 기밀에 대한 관심으로 디바이스 위험성이 높아지고 있다. 스마트 팩토리의 보안 위협 중에서 디바이스에 대한 보안위협 대상과 공격 유형은 다음과 같다.

1) 보안위협 대상 분석

스마트 팩토리 내에서 디바이스 보안 위협의 대상은 하드웨어, 소프트웨어, 센서, 액츄에이터 등이 있다. 하드웨어는 피지컬 컴포넌트를 의미하며 소프트웨어는 사물인터넷 디바이스의 운영체제, 펌웨어, 응용프로그램 등으로 이루어진다. 센서는 이벤트를 감지하고 정보를 전달하는 기능을 수행하며 액츄에이터는 사물인터넷 디바이스의 출력 유닛에 해당한다.

2) 공격 유형 분석

2009년 이후로 사물인터넷에서 빈번히 발생하고 있는 보안 공격은 DDos공격, hijacked공격, ransom 공격 등이 있다. 또한 2017년 3월에 사물인터넷 디바이스에서 DDOs 공격의 한 종류인 BrickerBot 공격이 발생한 사례가 있다. 가장 최근 발생하는 공격들을 살펴보면 Sandworm 공격, RootPipe 취약성, Shellshck 취약성, PasswordManager 취약성 등이 있다. Sandworm 공격은 악의적인 파일들이 컴퓨터에서 실행되면 자동으로 공격자의 컴퓨터에서 .gif 파일을 다운로드 하게 되고 .inf 파일이 동작될 때 다운로드 된 .gif 파일 .exe 파일로 이름이 변경되어 exe 파일로 추가되어 “registry runonce”에 저장된다. 그리고 그 이후 컴퓨터가 리부팅 되었을 때 저장된 몰웨어가 실행이 되며 피해를 입게 된다[5].

ROOTPIPE 취약성은 애플사가 2011에 데이터와 퍼미션을 주는 파일을 만들기 위해 OSX(writeconfig XPC) 서비스를 추가하면서 생겨난 공격 형태이다. 시스템 환경설정이나 컴맨드라인 툴을 지원하기 위해 생겨났는데 스웨덴의 "TrueSec AB"라는 사람에 의해 writeconfig OSX가 실행 시 공격에 취약하다는 것을 처음 발견하였다. 시스템 환경 등을 설정하기 위해 사용하는 파일을 생성하는 XPC 서비스 등을 이용하는 RootPipe 공격은 그림5에서와 같이 writeconfig XPC 서비스가 실행되면서 root 퍼미션과 SUID 파일을 변경할 수 있는 새로운 악의적인 파일을 만들고 실행하여 공격을 하게 된다.

Trend Micro의 원격 명령 실행에서 발견된 PASSWORD Manager 취약성은 2016년 5월에 구글의 Tavis에 의해 처음 발견되었다. Trand Micro의 PASSWORD Manager는 Javascript로 쓰여지고 multiple HTTP RPC 포트로 API가 동작한다. 대부분의 유저들이 웹 브라우저를 통해 공개된 API를 요청을 하게 되는데 이때 실행되어 공격을 하는 형태를 의미한다.

3) 디바이스 통신보안

-CoAP, LwM2M 보안

사물인터넷 서비스 구성을 위해 디바이스 간 통신에서 사용되는 프로토콜은 CoAP (Constrained Application Protocol)과 LwM2M(Ligh Weigh Machine to Machine) 두 가지가 있다. CoAP은 제한적 자원을 가지는 디바이스와 HTTP 기반의 응용 서비스 간 통신에 중점을 둔 프로토콜로 REST(Representational State Transfer) 통신이 가능하고, 응용계층 프로톨콜인 HTTP로 변환시켜 웹 서비스 디바이스를 쉽게 통합할 수 있다. CoAP에서의 보안을 위한 표준으로 DTLS(Datagram Transport Layer SEcurity)사용을 제안하고 있다. 하지만 표준에서 권고하는 보안기술의 많은 제약점으로 인해 실제 서비스에서 CoAP를 사용하기 위해선 보안 측면의 개선이 필요하다.

- MQTT 보안

MQTT(Message Queueing Telemetly Transport)

프로토콜도 사물인터넷 서비스 환경에 특화된 프로토콜로서 이 기종 기기 및 서비스 간 통신에 사용되고 있다. MQTT 표준문서에서는 구체적 암호알고리즘이나 보안 프로토콜이 정의되어 있지 않고 보안 요구사항을 정의함으로ㅆ 서비스 제공자에게 보안을 위한 책임을 부여하고 있다. 실제 구현 시 사용자와 디바이스에 대하 ㄴ인증메커니즘을 구체화할 필요가 있고 자원에 대한 접근제어, 통신 메시지의 무결성과 프라이버시 보호를 위한 기법도 정의될 필요가 있다.

4) 스마트 팩토리 공격 대응 방안

다양한 디바이스 공격들에 대응하기 위해서는 사물인터넷 네트워크(WAN:Wide Area Network)와 디바이스 M2M네트워크(LAN:Local Area Network)를 분리하여 게이트웨이/라우터를 위치시키는 구조가 요구된다. 이때 게이트웨이는 WAN과 LAN 사이에서 중재자 역할을 하게 된다. 센서가 연결된 디바이스나 액츄에이터는 WAN과 분리되어 있으며 게이트웨이를 통해 통신하거나 LAN의 라우터에 연결된다. 그림 4는 LAN과 WAN 사이의 구축된 게이트웨이-엣지 구조를 나타낸다[7].

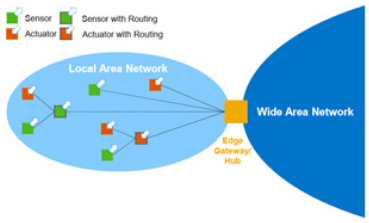

그림 4.게이트웨이-엣지 구조

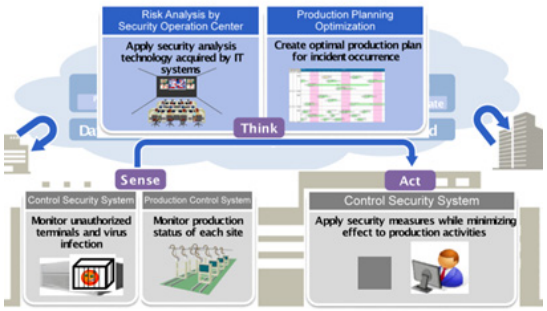

그림 5.스마트 팩토리 보안위협 대처 구조

센서가 연결된 디바이스와 액츄에이터를 모니터링하기 위한 보안 통제 시스템을 운영하고 위협 발생 시 대응하기 위한 구조가 구축되어야 한다. 그림 5의 보안콘트롤 시스템은 게이트웨이에 연결된 디바이스 및 액츄에이터 등을 모니터링하고, 만약 허가받지 않은 터미널의 접속이나 바이러스 침투가 발견되면 보안통제센터의 위협분석 기능을 통해 공격 및 위협의 종류를 가려낸다. 최상위 보안통제시스템에서는 위협의 결과를 최소화하기 위한 조치를 취할 결정을 하게 된다. 그림 5은 이러한 보안위협 대처 방안을 3단계(Sense/Think/Act)로 나누어 설명하고 있다.

III. 결 론

본 논문에서는 4차 산업혁명의 핵심 기술인 스마트 팩토리의 보안 기술과 요구사항에 대해 분석하고 그중에서 가장 보안 위협이 높은 디바이스의 보안 위협에 대해 분석하였다. 분석한 보안 위협에 대응하기 위한 디바이스 프로토콜과 보안 대응방안에 대하여도 제안하였다. 향후 디바이스 공격 뿐만 아니라 네트워크 공격, 어플리케이션 공격, 플랫폼 공격 등에 대한 상세한 위협을 분석하고 이에 대한 대응 방안을 제시하는 것이 필요하다.

참고문헌

[1] Industry 4.0 WorkingGroup, "Recommendations for implementing the strategic initiative Industrie 4.0", April 2013.
[2] 송하덕 외2인, “인더스트리 4.0 표준분석 및 한국의 스마트공장 표준화”, Joutnal of Standards and standardization, Vol 6, No 4, Dec 2016.
[3] Techncal Report of TEC, "MachinetoMachine Communication/IoT",V12, 29th, June, 2017.
[4] 허신욱 외3인, “스마트공장 보안성강화를 위한 제어시스템 보안기술”, 정보보호학회지, 제27권 제2호, 2017년.
[5] enisa, "Baseline Security Recommendations for IoT", November 2017".
[6] snsilo’s research paper, "VULNERABLE BY DESIGN: WHY DESTRUCTIVE EXPLOITS KEEP ON COMING", Feb, 2016.
[7] IEC, "IoT 2020:Smart and securite IoT Platform", IEC White paper